University of Maryland
CMSC858K — Introduction to Cryptography
Professor Jonathan Katz

Problem Set 2

Due at the *beginning* of class on Feb. 22

Please type your solutions, preferably using latex (if you are ever going to publish a paper, you will need to learn latex anyway...).

1. Construct a private-key encryption scheme that is indistinguishable for *arbitrary-length* messages, but only when used once. (I.e., it satisfies single-message indistinguishability but not multi-message indistinguishability.) You may assume the existence of PRGs and/or PRFs.

2. In class we defined security against *chosen-plaintext attacks*. Construct a private-key encryption scheme that is secure in the sense of multi-message indistinguishability, but is *not* secure against chosen-plaintext attacks. (*Hint:* it will not be a 'natural' scheme.)

3. Recall that in counter mode encryption, a message $m = m_1 \| \cdots \| m_\ell$ is encrypted under key k by choosing a random nonce r and outputting the ciphertext

$$r,\ m_1 \oplus F_k(r),\ \ldots,\ m_\ell \oplus F_k(r+\ell-1).$$

   Prove that counter mode encryption is secure in the sense of multi-message indistinguishability. For the purposes of this question, you may assume that the adversary always outputs two vectors containing $q(n)$ messages, and each message contains $\ell(n)$ message blocks.

4. Show that CBC-MAC is not a secure message authentication code when an adversary can obtain authentication tags on messages of different lengths.

5. Consider the following variant of CBC-MAC: The sender and receiver share a secret key k of length $\ell(n) \cdot n$, viewed as a vector of keys $k = \langle k_1, \ldots, k_\ell \rangle$ with $|k_i| = n$ for all i. Let $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a pseudorandom function. To authenticate a message m, the parties do the following:

   - Let $|m| = j \cdot n$, with $1 \leq j \leq \ell$. (If the message is too long, or its length is not a multiple of n, no authentication tag is computed.)
   - Compute the CBC-MAC on m using key k_j.

   (a) Is this scheme secure (when the adversary can obtains authentication tags on messages of different lengths) or not? If not, show an attack. If yes, give a proof (in this case you may assume security of CBC-MAC for *fixed-length* messages only).

   (b) Suggest a way to reduce the key size to n bits, while simultaneously allowing the scheme to be used for messages of *unbounded* length (as long as the length is a multiple of n).